
THE INSTITUTE OF INTERNAL AUDITORS
INTERNATIONAL CONFERENCE
VANCOUVER, BC, CANADA / JULY 5-8, 2015
VANCOUVER2015
Driving Value and Relevance by Objectively Quantifying Audit Findings and Control Assurance
Kevin Moylan – Strategic Risk Officer, Cathay Bank
Dan Zitting – VP of Product, ACL
Mountains of Change...Oceans of Opportunities

I’m Kevin, and I am not an Auditor.

My Job:

- Oversight of management of risk across a large, complex global banking organization
- I’m here today to convince auditors of two things:

1. Avoid audit findings with “open to interpretation” severity ratings
2. Objectively quantify and clearly articulate the level of assurance we have over risk in business operations

My Goal:

- To share with you today our journey that has aligned audit with our strategic risk agenda
  - One that is delivering us much more added value

What We've Accomplished

- A way to systematically assess risk across the Bank
- Use data to drive alignment and value from our audit results
- Making both myself and my counterparts in audit more strategically important:
  - A very clear system to objectively collaborate, identify and mitigate risk
  - Auditors able to provide our Board assurance on the effectiveness of those activities
  - A distinct clarity on overall risk assurance levels
  - Provides executive management *real* risk intelligence
    - Reliable intelligence used to make strategic decisions that is quantified, defensible, and supported by Internal Audit assurance

About our Environment

- NASDAQ traded Commercial Bank
  - 57 years; first Chinese-American Bank
  - 3rd largest California-based Bank
  - Managing over $12 billion in assets
  - Presence across the US, Hong Kong, Taipei, Shanghai and Beijing
- 7 teams supporting overall Governance, Risk, and Compliance
  - ERM, Internal Audit, InfoSec, IT Governance, AML, Compliance, and HR

Key Executive / Board Expectations

1. Integrity in everything we do – a company value
2. Successfully navigate the highly complex regulatory environment for multi-jurisdiction banking organization
3. Acutely manage key risk areas including liquidity, credit, capital, IT, Info security, reputation, etc.
4. Provide clear, understandable insight into the state of the risk environment to enable risk-intelligent business decisions
5. Enable safe risk taking so we can drive performance

My Vision

An enterprise-wide coordinated, ERM-led, cross functional team-based approach to risk management that enables the Bank to take risk intelligently, enabling optimized performance:

- Consolidated KRIs (with assurance from internal audit) across all operations that deliver simple, clear, and meaningful risk intelligence
- Focused, elegant technology enablement that empowers the full range of teams to capture information in a consistent way to enable consistent, cross functional risk assurance KRIs

Where Assurance Activities Fall Down

- Teams may not understand full strategic risk landscape and may limit focus to areas that don't encompass critical risk areas
  - i.e. interdependencies (upstream, downstream, cross-stream, etc.); perceived risk vs. actual (auditing functions perceived to be worrisome, but not)
- In process areas selected for review, often findings identified are rated essentially judgmentally, not reflective of the up-front risk analysis and, in turn, the degree of importance of the controls tested
  - i.e. a finding is rated "high" when the control it is related to mitigates only low rated risks (the finding was likely rated judgmentally relative to the control, rather than to the risks the control was created to manage)
- Findings identified, and audit reports in general, are stated in ways that don't fairly communicate the true (quant) state of risk exposure
  - i.e. they communicate the severity of the finding, not the overall risk exposure in the process area

Our Solution Approach

- Agree and align on an integrated ERM approach across teams through our governance committees
  - Including risk appetite, lexicon, quantitative & qualitative risk scores / values, etc.
- Agree and align on the KRIs delivered
  - And a consistent methodology to create them
- Leverage our GRC technology platform to automate the creation and delivery of the KRIs by process area
  - As daily audit, risk, and compliance work activities are performed & completed

Kevin is my favorite client (at least that is what I tell him)

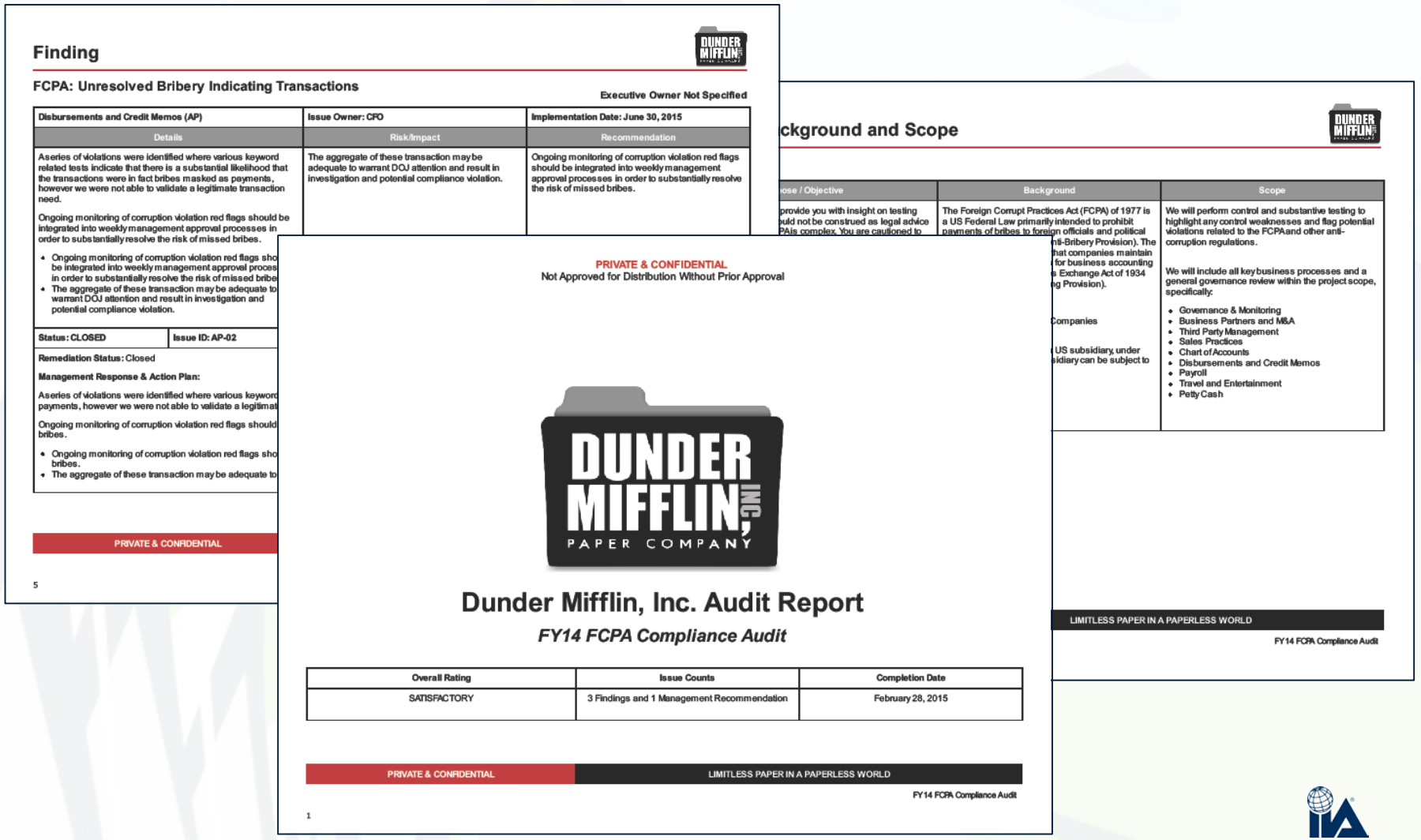
- My role is running product strategy and product design for ACL, but – unlike Kevin – 10 years an auditor
- Kevin had purchased our ACL GRC platform to be the technology backbone for implementing his vision
- We love Cathay Bank because of Kevin's big vision and our joint opportunity to make a big impact for the Bank's management and board
  - We always want to invest like crazy in these kinds of clients

The fundamental goal

Objectively calculating an overall KRI that tells a clear story on the state of a business process or objective… in one, simple figure

1. Same methodology can translate objectively quantified severity ratings where audit findings are identified
2. Build dashboards that aggregates the same KRI for multiple processes to create complete views of risk assurance
3. Easy and automated – created and updated automatically, in real-time, as daily tasks are completed

Essentially, summarizing this…



Finding

FCPA: Unresolved Bribery Indicating Transactions

Executive Owner Not Specified

Disbursements and Credit Memos (AP)	Issue Owner: CFO	Implementation Date: June 30, 2015
Details	Risk/Impact	Recommendation
A series of violations were identified where various keyword related tests indicate that there is a substantial likelihood that the transactions were in fact bribes masked as payments, however we were not able to validate a legitimate transaction need. Ongoing monitoring of corruption violation red flags should be integrated into weekly management approval processes in order to substantially resolve the risk of missed bribes.	The aggregate of these transaction may be adequate to warrant DOJ attention and result in investigation and potential compliance violation.	Ongoing monitoring of corruption violation red flags should be integrated into weekly management approval processes in order to substantially resolve the risk of missed bribes.

- Ongoing monitoring of corruption violation red flags sho
  be integrated into weekly management approval proces
  in order to substantially resolve the risk of missed bribe
- The aggregate of these transaction may be adequate to
  warrant DOJ attention and result in investigation and
  potential compliance violation.

Status: CLOSED	Issue ID: AP-02

Remediation Status: Closed

Management Response & Action Plan:

A series of violations were identified where various keyword
payments, however we were not able to validate a legitimat

Ongoing monitoring of corruption violation red flags should
bribes.

- Ongoing monitoring of corruption violation red flags sho
  bribes.
- The aggregate of these transaction may be adequate to

PRIVATE & CONFIDENTIAL

5

ckground and Scope

ose / Objective	Background	Scope
provide you with insight on testing uld not be construed as legal advice PAIs complex. You are cautioned to	The Foreign Corrupt Practices Act (FCPA) of 1977 is a US Federal Law primarily intended to prohibit payments of bribes to foreign officials and political ni-Bribery Provision). The hat companies maintain for business accounting Exchange Act of 1934 g Provision).	We will perform control and substantive testing to highlight any control weaknesses and flag potential violations related to the FCPA and other anti-corruption regulations. We will include all key business processes and a general governance review within the project scope, specifically: • Governance & Monitoring • Business Partners and M&A • Third Party Management • Sales Practices • Chart of Accounts • Disbursements and Credit Memos • Payroll • Travel and Entertainment • Petty Cash
Companies		
US subsidiary, under sidiary can be subject to		

LIMITLESS PAPER IN A PAPERLESS WORLD

FY14 FCPA Compliance Audit

PRIVATE & CONFIDENTIAL
Not Approved for Distribution Without Prior Approval

DUNDER MIFFLIN, INC
PAPER COMPANY

Dunder Mifflin, Inc. Audit Report

FY14 FCPA Compliance Audit

Overall Rating	Issue Counts	Completion Date
SATISFACTORY	3 Findings and 1 Management Recommendation	February 28, 2015

PRIVATE & CONFIDENTIAL | LIMITLESS PAPER IN A PAPERLESS WORLD

FY14 FCPA Compliance Audit

1

…into this (while removing subjectivity)

Designing a solution

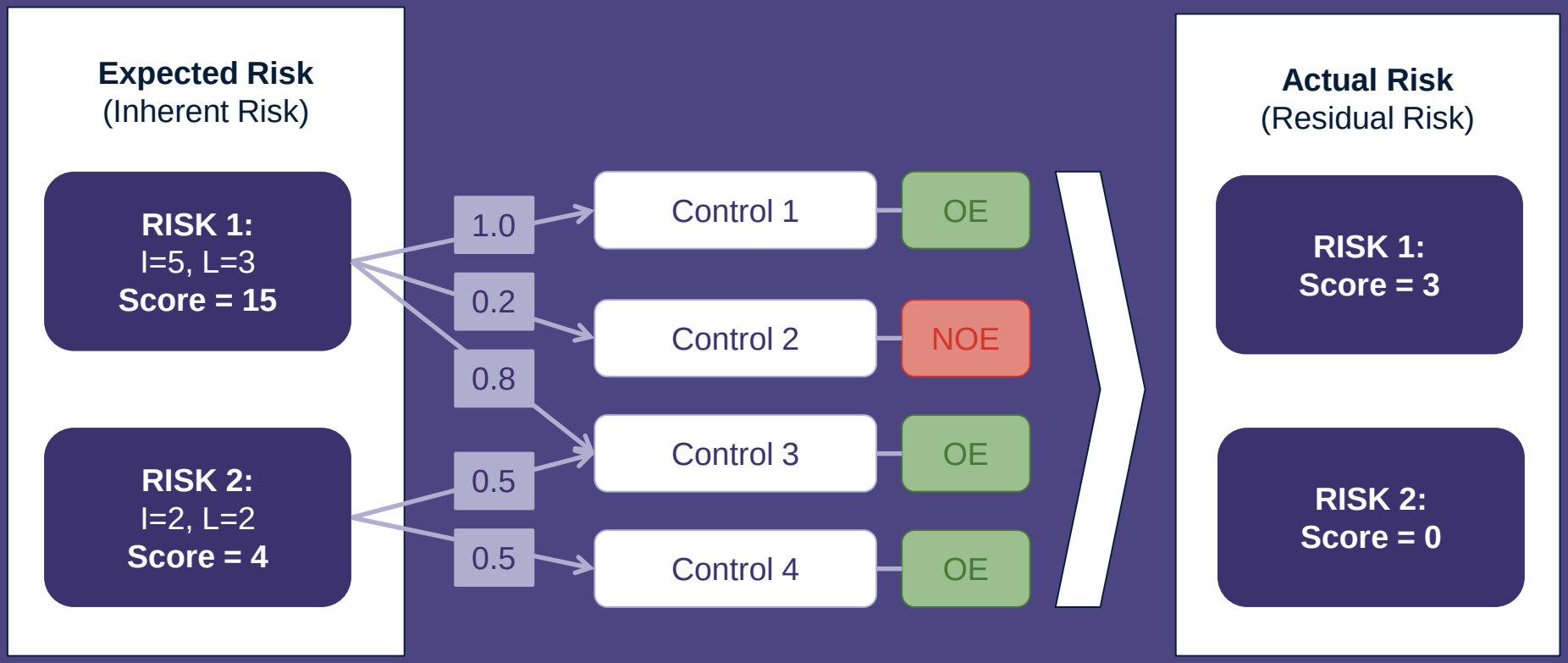
Clearly a very solvable problem, based on the simple constructs of properly structured risk/control frameworks.

Step 1 – Defining an objective quantification algorithm

Keys to success:

- A simple, understandable algorithm that will be broadly supported
- Quantification driven by up-front risk scoring and weighting only
- Outcome/deliverable is a single, easily digestible KRI metric

OBJECTIVELY QUANTIFIED RISK ASSURANCE FOR A GIVEN PROCESS/OBJECTIVE



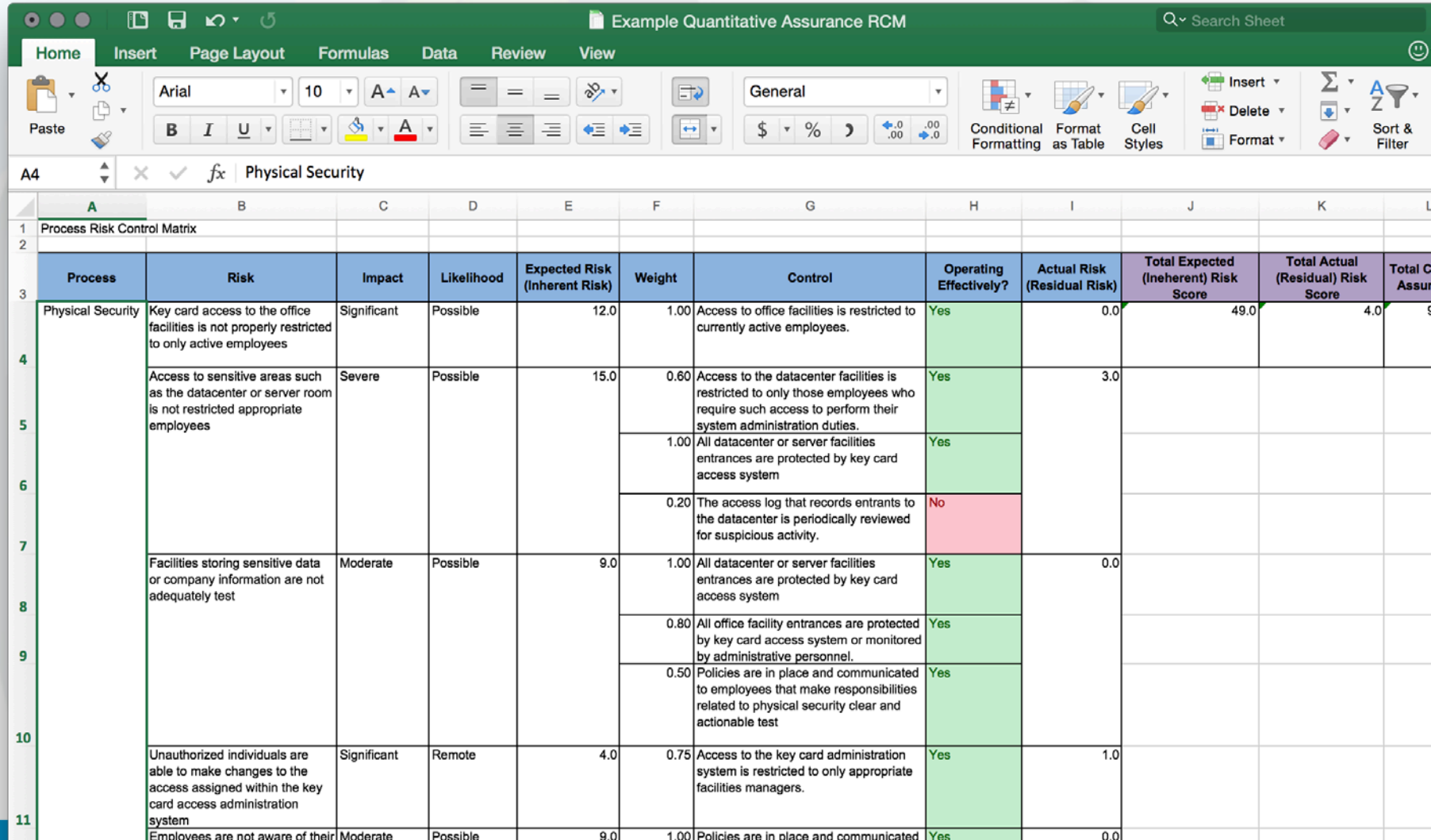
Total Expected Risk Score = 19
Total Actual Risk Score = 3
Total Risk Assurance = 84%

Step 1 – Outcome KRI

- Simple, visual, fully quantified indicator for process control effectiveness
- Aggregate scores to measure by:
  - Audit
  - Entity
  - Enterprise Risk

Step 1 – Test drive our method

http://enablement.aclgrc.com/Quantitative_Assurance_RCM.xls



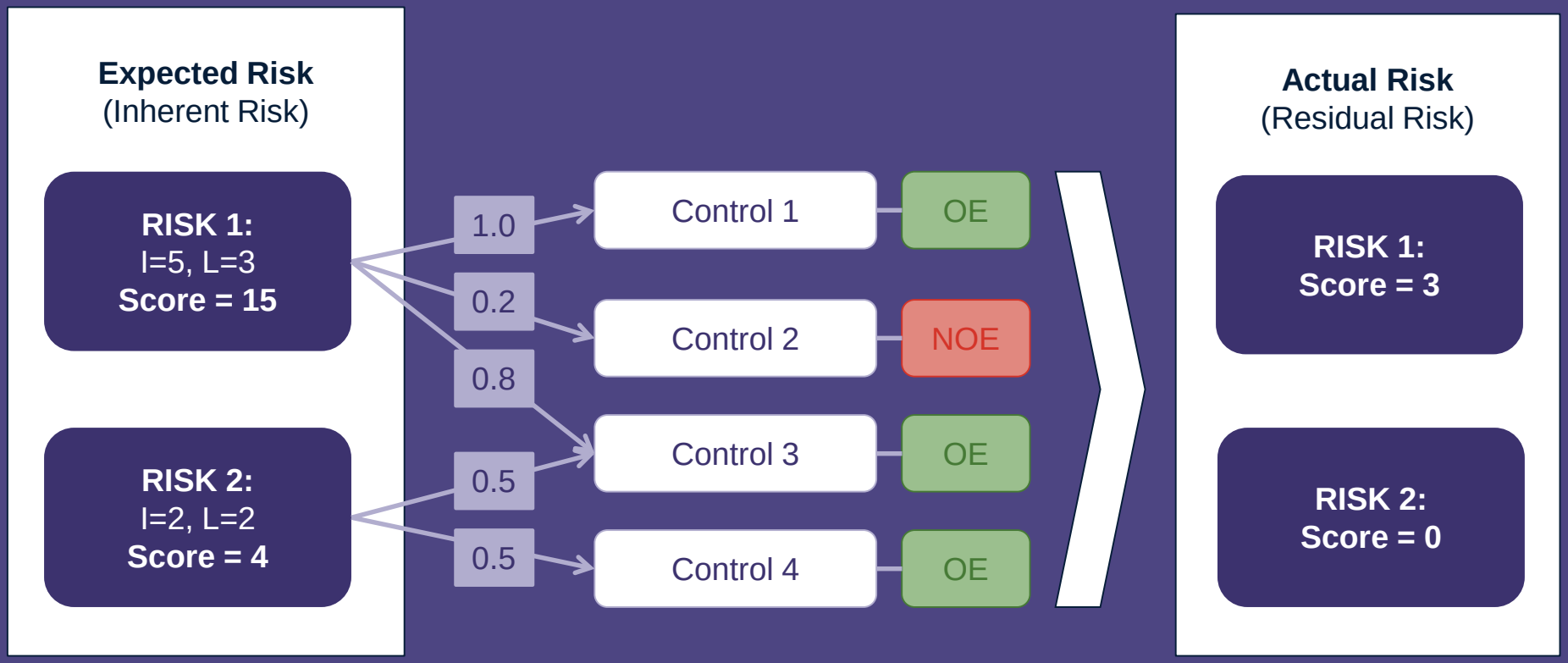
Process Risk Control Matrix

Process	Risk	Impact	Likelihood	Expected Risk (Inherent Risk)	Weight	Control	Operating Effectively?	Actual Risk (Residual Risk)	Total Expected (Ineherent) Risk Score	Total Actual (Residual) Risk Score	Total C Assur
Physical Security	Key card access to the office facilities is not properly restricted to only active employees	Significant	Possible	12.0	1.00	Access to office facilities is restricted to currently active employees.	Yes	0.0	49.0	4.0	
	Access to sensitive areas such as the datacenter or server room is not restricted appropriate employees	Severe	Possible	15.0	0.60	Access to the datacenter facilities is restricted to only those employees who require such access to perform their system administration duties.	Yes	3.0			
					1.00	All datacenter or server facilities entrances are protected by key card access system	Yes				
					0.20	The access log that records entrants to the datacenter is periodically reviewed for suspicious activity.	No				
	Facilities storing sensitive data or company information are not adequately test	Moderate	Possible	9.0	1.00	All datacenter or server facilities entrances are protected by key card access system	Yes	0.0			
					0.80	All office facility entrances are protected by key card access system or monitored by administrative personnel.	Yes				
					0.50	Policies are in place and communicated to employees that make responsibilities related to physical security clear and actionable test	Yes				
	Unauthorized individuals are able to make changes to the access assigned within the key card access administration system	Significant	Remote	4.0	0.75	Access to the key card administration system is restricted to only appropriate facilities managers.	Yes	1.0			
	Employees are not aware of their	Moderate	Possible	9.0	1.00	Policies are in place and communicated	Yes	0.0			

Step 2 – Rate findings accordingly

- When controls fail and audit findings are identified, rate severity based only on the impact to overall process risk assurance
  - Weighting / scoring pre-negotiated up front with the auditor and auditee
  - This ensures they are rated relative to risk assessment, rather than in a judgmental vacuum
- Consider eliminating high/medium/low sorts of severity ratings all together and instead simply report the “negative risk assurance impact”

USING OUR EARLIER EXAMPLE…



Total expected risk score = 19
Total actual risk score = 3
Total risk assurance = 84%

Audit finding = "We noted control 2 was not operating effectively…"
Severity = -16% risk assurance

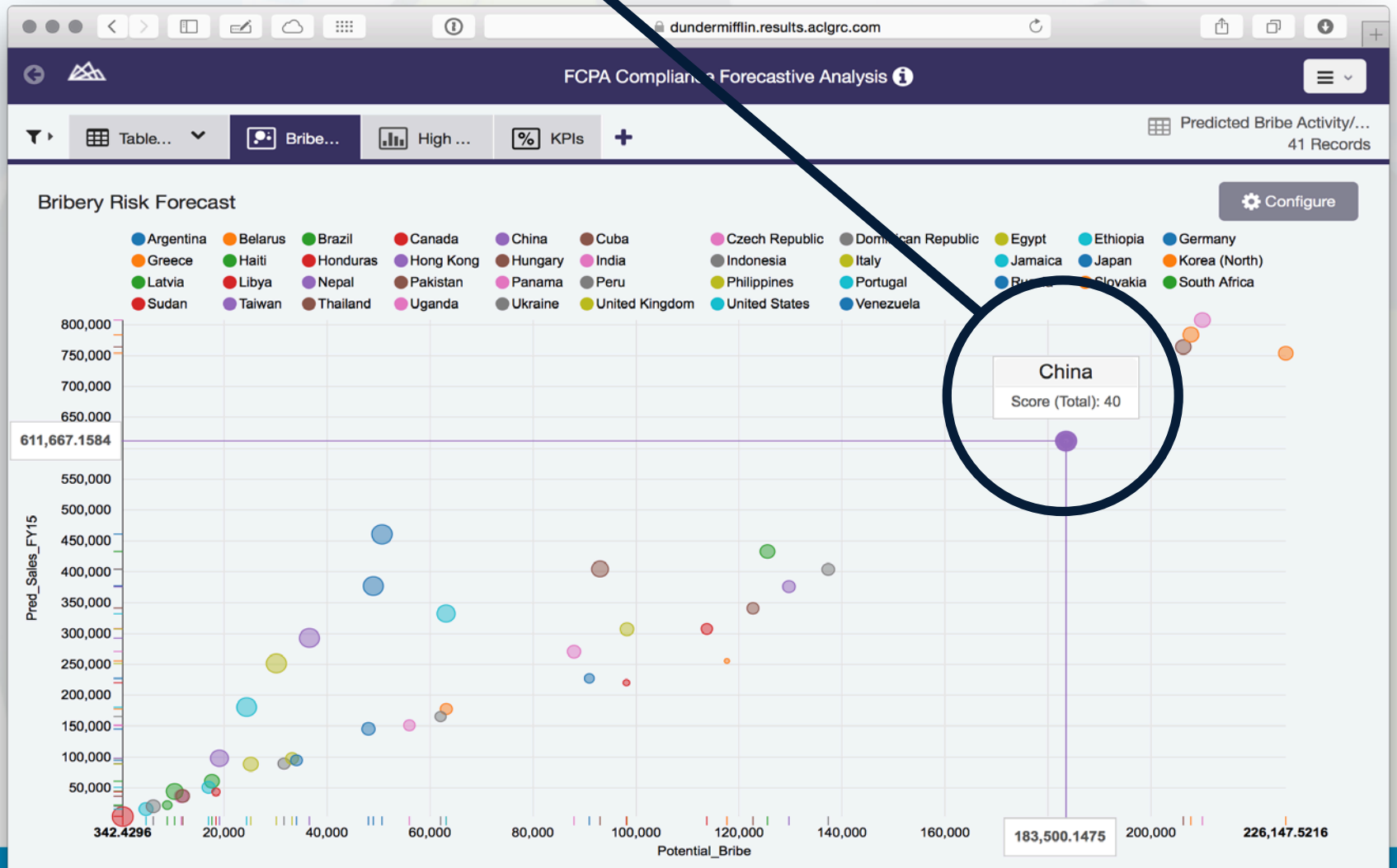
Step 3 – Go fully data-driven

Keys to success:

- Replace judgment-based risk ratings with measurements from objective datasets
  - First choice for objective measurement datasets should be results from data analytics
  - Second choice for objective measurement datasets should be human survey results
  - Best of all, leverage both through dataset blending
- Once you've set risk ratings based on objective datasets, continue with process in steps 1 & 2

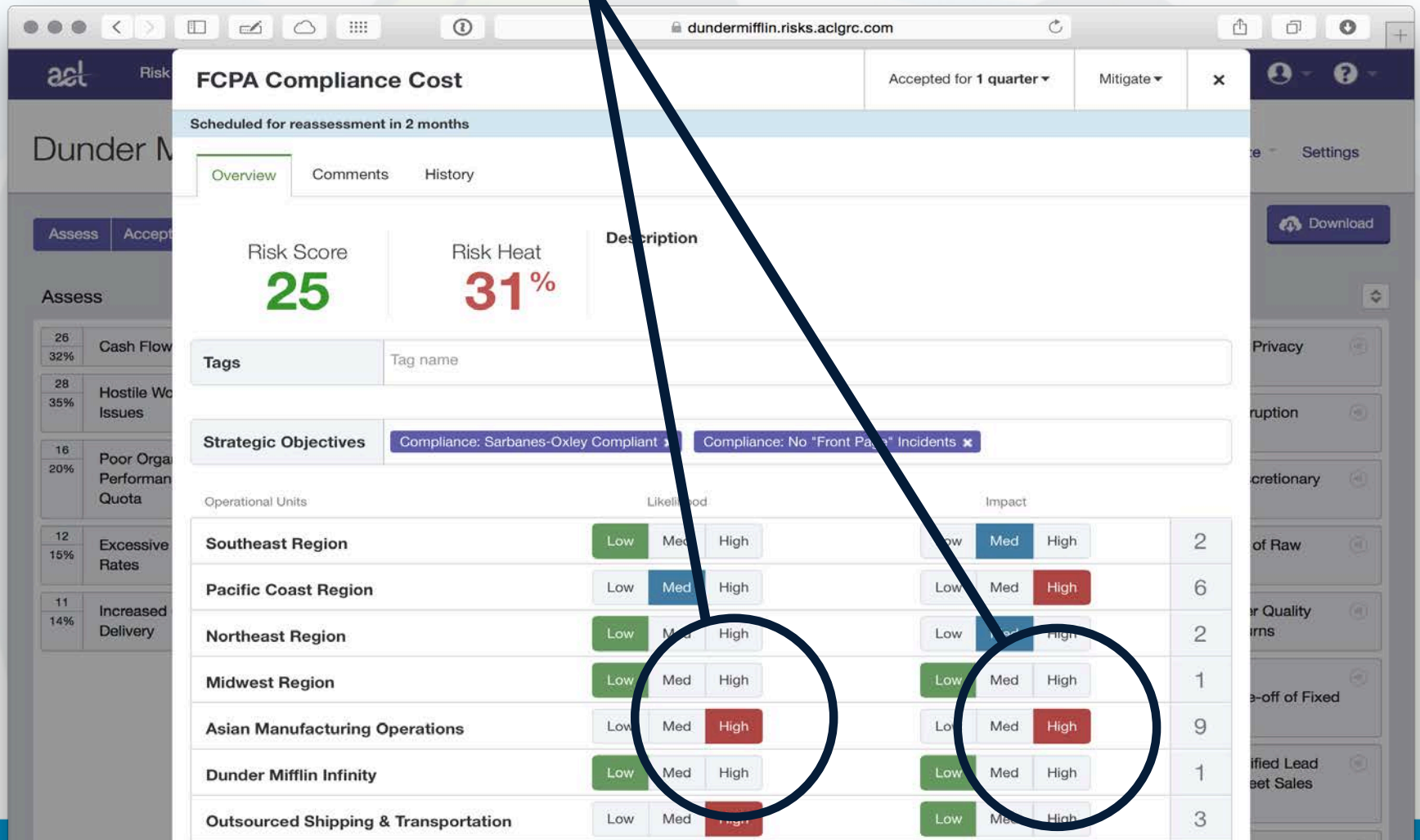
Step 3 – Go fully data-driven

Basic predictive risk analytics like this



Step 3 – Go fully data-driven

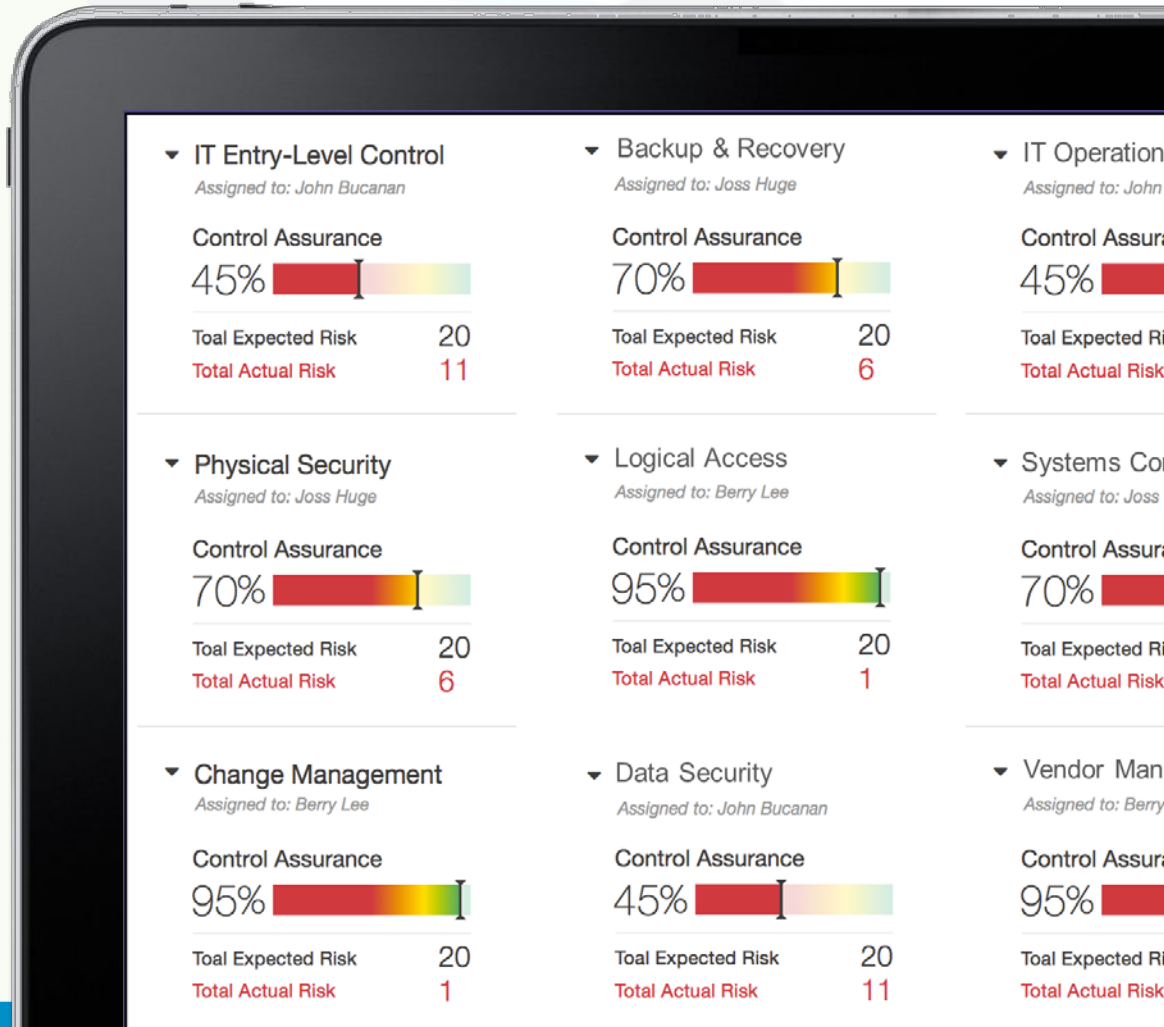
Drives a risk scoring exercise like this (thus removing judgment)



Step 4 – Deliver risk assurance intelligence across operations

Keys to success:

- KRIs delivered in real-time, anytime
- KRIs delivered in the way top leaders consume
- Breadth of operational KRI coverage



Step 4 – Outcome

- Straight forward, timely risk intelligence (with assurance from audit) that enables safe risk taking
  - Taking risk drives performance… enabling safe risk taking enables reliably higher performance

- Drive your value and relevance toward the vision of becoming the most sought-after in your organization

What we've implemented

- Worked with ACL to design the algorithm and have implemented in our processes (Step 1)
- Worked with internal audit to align reporting on audit finding ratings to the overall impact on a processes risk assurance level (Step 2)
  - Added feedback loop from Internal Audit on any missing controls or control deficiencies
- Created consolidated dashboard to report to executive management and the board our risk assurance KRIs (Step 4)

Our roadmap

1. Finish spreading the unified risk assessment and validation process through the remaining GRC-related teams
2. Attain full coverage on the breadth of our core operational processes across the bank (currently ~60% coverage)
3. Implement fully data-driven assessments of risks…prioritized order based on current risk ratings

Key benefits realized

1. Executive management cares about what we're producing and feels like they have risk intelligence and confidence that they can use to drive decisions
2. The board cares about what we're producing and feels like they have ASSURANCE around key risk areas they can use to continue to rely on management to move the business safely forward

Key benefits realized

3. We can quantify a “risk assurance ROI” (risk assurance gained per $X spent) for investments made in the various risk management functions around the bank
4. My personal career benefits and experience gained from being able to use this initiative to drive GRC integration and consistent value delivery cross-functionally in front of exec management and the board

Linkedin – Dan Zitting, VP of Product at ACL

Linkedin – Kevin Moylan, Strategic Risk Officer at Cathay Bank

QUESTIONS?